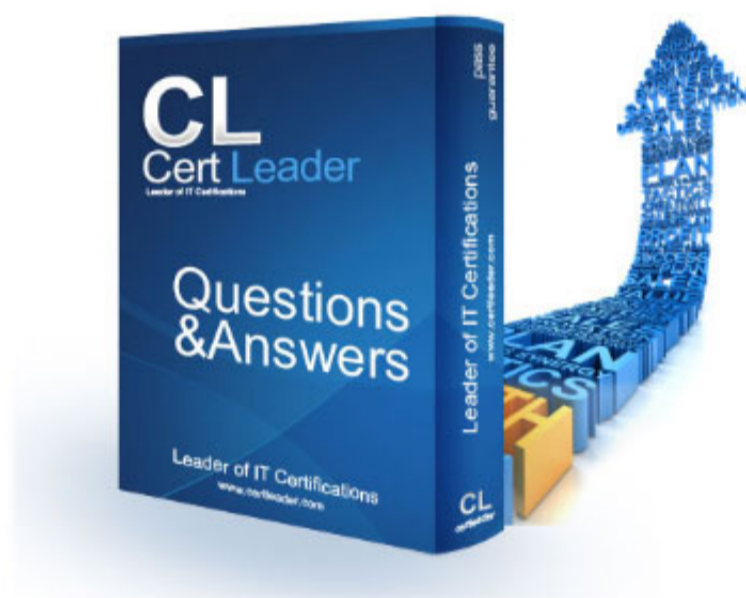


## AWS-Certified-Solutions-Architect-Professional Dumps

### Amazon AWS Certified Solutions Architect Professional

<https://www.certleader.com/AWS-Certified-Solutions-Architect-Professional-dumps.html>



**NEW QUESTION 1**

- (Exam Topic 2)

An external audit of a company's serverless application reveals IAM policies that grant too many permissions. These policies are attached to the company's AWS Lambda execution roles. Hundreds of the company's Lambda functions have broad access permissions, such as full access to Amazon S3 buckets and Amazon DynamoDB tables. The company wants each function to have only the minimum permissions that the function needs to complete its task.

A solutions architect must determine which permissions each Lambda function needs.

What should the solutions architect do to meet this requirement with the LEAST amount of effort?

- A. Set up Amazon CodeGuru to profile the Lambda functions and search for AWS API call
- B. Create an inventory of the required API calls and resources for each Lambda function
- C. Create new IAM access policies for each Lambda function
- D. Review the new policies to ensure that they meet the company's business requirements.
- E. Turn on AWS CloudTrail logging for the AWS account
- F. Use AWS Identity and Access Management Access Analyzer to generate IAM access policies based on the activity recorded in the CloudTrail log
- G. Review the generated policies to ensure that they meet the company's business requirements.
- H. Turn on AWS CloudTrail logging for the AWS account
- I. Create a script to parse the CloudTrail log, search for AWS API calls by Lambda execution role, and create a summary report
- J. Review the report
- K. Create IAM access policies that provide more restrictive permissions for each Lambda function.
- L. Turn on AWS CloudTrail logging for the AWS account
- M. Export the CloudTrail logs to Amazon S3. Use Amazon EMR to process the CloudTrail logs in Amazon S3 and produce a report of API calls and resources used by each execution role
- N. Create a new IAM access policy for each role
- O. Export the generated roles to an S3 bucket
- P. Review the generated policies to ensure that they meet the company's business requirements.

**Answer: B**

**Explanation:**

IAM Access Analyzer helps you identify the resources in your organization and accounts, such as Amazon S3 buckets or IAM roles, shared with an external entity. This lets you identify unintended access to your resources and data, which is a security risk. IAM Access Analyzer identifies resources shared with external principals by using logic-based reasoning to analyze the resource-based policies in your AWS environment.

<https://docs.aws.amazon.com/IAM/latest/UserGuide/what-is-access-analyzer.html>

**NEW QUESTION 2**

- (Exam Topic 2)

A company has deployed its database on an Amazon RDS for MySQL DB instance in the us-east-1 Region. The company needs to make its data available to customers in Europe. The customers in Europe must have access to the same data as customers in the United States (US) and will not tolerate high application latency or stale data. The customers in Europe and the customers in the US need to write to the database. Both groups of customers need to see updates from the other group in real time.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL replica of the RDS for MySQL DB instance
- B. Pause application writes to the RDS DB instance
- C. Promote the Aurora Replica to a standalone DB instance
- D. Reconfigure the application to use the Aurora database and resume write
- E. Add eu-west-1 as a secondary Region to the DB instance
- F. Enable write forwarding on the DB instance
- G. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.
- H. Add a cross-Region replica in eu-west-1 for the RDS for MySQL DB instance
- I. Configure the replica to replicate write queries back to the primary DB instance
- J. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- K. Copy the most recent snapshot from the RDS for MySQL DB instance to eu-west-1. Create a new RDS for MySQL DB instance in eu-west-1 from the snapshot
- L. Configure MySQL logical replication from us-east-1 to eu-west-1. Enable write forwarding on the DB instance
- M. Deploy the application in eu-west-1. Configure the application to use the RDS for MySQL endpoint in eu-west-1.
- N. Convert the RDS for MySQL DB instance to an Amazon Aurora MySQL DB instance
- O. Add eu-west-1 as a secondary Region to the DB instance
- P. Enable write forwarding on the DB instance
- Q. Deploy the application in eu-west-1. Configure the application to use the Aurora MySQL endpoint in eu-west-1.

**Answer: D**

**Explanation:**

The company should use AWS Amplify to create a static website for uploads of media files. The company should use Amplify Hosting to serve the website through Amazon CloudFront. The company should use Amazon S3 to store the uploaded media files. The company should use Amazon Cognito to authenticate users. This solution will meet the requirements with the least operational overhead because AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS, with the flexibility to leverage the breadth of AWS services as use cases evolve. No cloud expertise needed<sup>1</sup>. By using AWS Amplify, the company can refactor the application to a serverless architecture that reduces operational complexity and costs. AWS Amplify offers the following features and benefits:

- Amplify Studio: A visual interface that enables you to build and deploy a full-stack app quickly, including frontend UI and backend.
- Amplify CLI: A local toolchain that enables you to configure and manage an app backend with just a few commands.
- Amplify Libraries: Open-source client libraries that enable you to build cloud-powered mobile and web apps.
- Amplify UI Components: Open-source design system with cloud-connected components for building feature-rich apps fast.
- Amplify Hosting: Fully managed CI/CD and hosting for fast, secure, and reliable static and server-side rendered apps.

By using AWS Amplify to create a static website for uploads of media files, the company can leverage Amplify Studio to visually build a pixel-perfect UI and connect it to a cloud backend in clicks. By using Amplify Hosting to serve the website through Amazon CloudFront, the company can easily deploy its web app or website to the fast, secure, and reliable AWS content delivery network (CDN), with hundreds of points of presence globally. By using Amazon S3 to store the uploaded media files, the company can benefit from a highly scalable, durable, and cost-effective object storage service that can handle any amount of data<sup>2</sup>. By

using Amazon Cognito to authenticate users, the company can add user sign-up, sign-in, and access control to its web app with a fully managed service that scales to support millions of users<sup>3</sup>.

The other options are not correct because:

➤ Using AWS Application Migration Service to migrate the application server to Amazon EC2 instances would not refactor the application or accelerate development. AWS Application Migration Service (AWS MGN) is a service that enables you to migrate physical servers, virtual machines (VMs), or cloud servers from any source infrastructure to AWS without requiring agents or specialized tools. However, this would not address the challenges of overutilization and data uploads failures. It would also not reduce operational overhead or costs compared to a serverless architecture.

➤ Creating a static website for uploads of media files and using AWS AppSync to create an API would not be as simple or fast as using AWS Amplify. AWS AppSync is a service that enables you to create flexible APIs for securely accessing, manipulating, and combining data from one or more data sources. However, this would require more configuration and management than using Amplify Studio and Amplify Hosting. It would also not provide authentication features like Amazon Cognito.

➤ Setting up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application would not be as suitable as using Amazon Cognito. AWS Single Sign-On (AWS SSO) is a service that enables you to centrally manage SSO access and user permissions across multiple AWS accounts and business applications. However, this service is designed for enterprise customers who need to manage access for employees or partners across multiple resources. It is not intended for authenticating end users of web or mobile apps.

References:

➤ <https://aws.amazon.com/amplify/>

➤ <https://aws.amazon.com/s3/>

➤ <https://aws.amazon.com/cognito/>

➤ <https://aws.amazon.com/mgn/>

➤ <https://aws.amazon.com/appsync/>

➤ <https://aws.amazon.com/single-sign-on/>

### NEW QUESTION 3

- (Exam Topic 2)

A company needs to optimize the cost of backups for Amazon Elastic File System (Amazon EFS). A solutions architect has already configured a backup plan in AWS Backup for the EFS backups. The backup plan contains a rule with a lifecycle configuration to transition EFS backups to cold storage after 7 days and to keep the backups for an additional 90 days.

After 1 month, the company reviews its EFS storage costs and notices an increase in the EFS backup costs. The EFS backup cold storage produces almost double the cost of the EFS warm backup storage.

What should the solutions architect do to optimize the cost?

- A. Modify the backup rule's lifecycle configuration to move the EFS backups to cold storage after 1 day. Set the backup retention period to 30 days.
- B. Modify the backup rule's lifecycle configuration to move the EFS backups to cold storage after 8 days. Set the backup retention period to 30 days.
- C. Modify the backup rule's lifecycle configuration to move the EFS backups to cold storage after 1 day. Set the backup retention period to 90 days.
- D. Modify the backup rule's lifecycle configuration to move the EFS backups to cold storage after 8 days. Set the backup retention period to 98 days.

**Answer:** A

#### Explanation:

The cost of EFS backup cold storage is \$0.01 per GB-month, whereas the cost of EFS backup warm storage is \$0.05 per GB-month<sup>1</sup>. Therefore, moving the backups to cold storage as soon as possible will reduce the storage cost. However, cold storage backups must be retained for a minimum of 90 days<sup>2</sup>, otherwise they incur a pro-rated charge equal to the storage charge for the remaining days<sup>1</sup>. Therefore, setting the backup retention period to 30 days will incur a penalty of 60 days of cold storage cost for each backup deleted. This penalty will still be lower than keeping the backups in warm storage for 7 days and then in cold storage for 83 days, which is the current configuration. Therefore, option A is the most cost-effective solution.

### NEW QUESTION 4

- (Exam Topic 2)

A company has VPC flow logs enabled for its NAT gateway. The company is seeing Action = ACCEPT for inbound traffic that comes from public IP address 198.51.100.2 destined for a private Amazon EC2 instance.

A solutions architect must determine whether the traffic represents unsolicited inbound connections from the internet. The first two octets of the VPC CIDR block are 203.0.

Which set of steps should the solutions architect take to meet these requirements?

- A. Open the AWS CloudTrail console
- B. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface
- C. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- D. Open the Amazon CloudWatch console
- E. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface
- F. Run a query to filter with the destination address set as "like 203.0" and the source address set as "like 198.51.100.2". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- G. Open the AWS CloudTrail console
- H. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface
- I. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.
- J. Open the Amazon CloudWatch console
- K. Select the log group that contains the NAT gateway's elastic network interface and the private instance's elastic network interface
- L. Run a query to filter with the destination address set as "like 198.51.100.2" and the source address set as "like 203.0". Run the stats command to filter the sum of bytes transferred by the source address and the destination address.

**Answer:** D

#### Explanation:

<https://aws.amazon.com/premiumsupport/knowledge-center/vpc-analyze-inbound-traffic-nat-gateway/> by Cloudxie says "select appropriate log"

**NEW QUESTION 5**

- (Exam Topic 2)

A company uses a load balancer to distribute traffic to Amazon EC2 instances in a single Availability Zone. The company is concerned about security and wants a solutions architect to re-architect the solution to meet the following requirements:

- Inbound requests must be filtered for common vulnerability attacks.
- Rejected requests must be sent to a third-party auditing application.
- All resources should be highly available. Which solution meets these requirements?

- A. Configure a Multi-AZ Auto Scaling group using the application's AM
- B. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target
- C. Use Amazon Inspector to monitor traffic to the ALB and EC2 instance
- D. Create a web ACL in WA
- E. Create an AWS WAF using the web ACL and AL
- F. Use an AWS Lambda function to frequently push the Amazon Inspector report to the third-party auditing application.
- G. Configure an Application Load Balancer (ALB) and add the EC2 instances as targets Create a web ACL in WA
- H. Create an AWS WAF using the web ACL and ALB name and enable logging with Amazon CloudWatch Log
- I. Use an AWS Lambda function to frequently push the logs to the third-party auditing application.
- J. Configure an Application Load Balancer (ALB) along with a target group adding the EC2 instances as target
- K. Create an Amazon Kinesis Data Firehose with the destination of the third-party auditing applicatio
- L. Create a web ACL in WA
- M. Create an AWS WAF using the web ACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destinatio
- N. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.
- O. Configure a Multi-AZ Auto Scaling group using the application's AM
- P. Create an Application Load Balancer (ALB) and select the previously created Auto Scaling group as the target
- Q. Create an Amazon Kinesis Data Firehose with a destination of the third-party auditing applicatio
- R. Create a web ACL inWA
- S. Create an AWS WAF using the WebACL and ALB then enable logging by selecting the Kinesis Data Firehose as the destinatio
- T. Subscribe to AWS Managed Rules in AWS Marketplace, choosing the WAF as the subscriber.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/waf/latest/developerguide/marketplace-managed-rule-groups.html>

**NEW QUESTION 6**

- (Exam Topic 2)

A company uses AWS Organizations to manage more than 1.000 AWS accounts. The company has created a new developer organization. There are 540 developer member accounts that must be moved to the new developer organization. All accounts are set up with all the required Information so that each account can be operated as a standalone account.

Which combination of steps should a solutions architect take to move all of the developer accounts to the new developer organization? (Select THREE.)

- A. Call the MoveAccount operation in the Organizations API from the old organization's management account to migrate the developer accounts to the new developer organization.
- B. From the management account, remove each developer account from the old organization using the RemoveAccountFromOrganization operation in the Organizations API.
- C. From each developer account, remove the account from the old organization using theRemoveAccountFromOrganization operation in the Organizations API.
- D. Sign in to the new developer organization's management account and create a placeholder member account that acts as a target for the developer account migration.
- E. Call the InviteAccountToOrganization operation in the Organizations API from the new developer organization's management account to send invitations to the developer accounts.
- F. Have each developer sign in to their account and confirm to join the new developer organization.

**Answer:** BEF

**Explanation:**

"This operation can be called only from the organization's management account. Member accounts can remove themselves with LeaveOrganization instead."

[https://docs.aws.amazon.com/organizations/latest/APIReference/API\\_RemoveAccountFromOrganization.html](https://docs.aws.amazon.com/organizations/latest/APIReference/API_RemoveAccountFromOrganization.html)

**NEW QUESTION 7**

- (Exam Topic 2)

A financial services company loaded millions of historical stock trades into an Amazon DynamoDB table. The table uses on-demand capacity mode. Once each day at midnight, a few million new records are loaded into the table. Application read activity against the table happens in bursts throughout the day. and a limited set of keys are repeatedly looked up. The company needs to reduce costs associated with DynamoDB.

Which strategy should a solutions architect recommend to meet this requirement?

- A. Deploy an Amazon ElastiCache cluster in front of the DynamoDB table.
- B. Deploy DynamoDB Accelerator (DAX). Configure DynamoDB auto scalin
- C. Purchase Savings Plans in Cost Explorer
- D. Use provisioned capacity mod
- E. Purchase Savings Plans in Cost Explorer.
- F. Deploy DynamoDB Accelerator (DAX). Use provisioned capacity mod
- G. Configure DynamoDB auto scaling.

**Answer:** D

**Explanation:**

<https://docs.aws.amazon.com/amazondynamodb/latest/developerguide/HowItWorks.ReadWriteCapacityMode.h>

**NEW QUESTION 8**

- (Exam Topic 2)

A company has developed a hybrid solution between its data center and AWS. The company uses Amazon VPC and Amazon EC2 instances that send application logs to Amazon CloudWatch. The EC2 instances read data from multiple relational databases that are hosted on premises. The company wants to monitor which EC2 instances are connected to the databases in near-real time. The company already has a monitoring solution that uses Splunk on premises. A solutions architect needs to determine how to send networking traffic to Splunk. How should the solutions architect meet these requirements?

- A. Enable VPC flows logs, and send them to CloudWatc
- B. Create an AWS Lambda function to periodically export the CloudWatch logs to an Amazon S3 bucket by using the pre-defined export function
- C. Generate ACCESS\_KEY and SECRET\_KEY AWS credential
- D. Configure Splunk to pull the logs from the S3 bucket by using those credentials.
- E. Create an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination
- F. Configure a pre-processing AWS Lambda function with a Kinesis Data Firehose stream processor that extracts individual log events from records sent by CloudWatch Logs subscription filter
- G. Enable VPC flows logs, and send them to CloudWatc
- H. Create a CloudWatch Logs subscription that sends log events to the Kinesis Data Firehose delivery stream.
- I. Ask the company to log every request that is made to the databases along with the EC2 instance IP address
- J. Export the CloudWatch logs to an Amazon S3 bucket
- K. Use Amazon Athena to query the logs grouped by database name
- L. Export Athena results to another S3 bucket
- M. Invoke an AWS Lambda function to automatically send any new file that is put in the S3 bucket to Splunk.
- N. Send the CloudWatch logs to an Amazon Kinesis data stream with Amazon Kinesis Data Analytics for SQL Application
- O. Configure a 1 -minute sliding window to collect the event
- P. Create a SQL query that uses the anomaly detection template to monitor any networking traffic anomalies in near-real time
- Q. Send the result to an Amazon Kinesis Data Firehose delivery stream with Splunk as the destination.

**Answer: B**

**Explanation:**

<https://docs.aws.amazon.com/firehose/latest/dev/creating-the-stream-to-splunk.html>

**NEW QUESTION 9**

- (Exam Topic 2)

A company's interactive web application uses an Amazon CloudFront distribution to serve images from an Amazon S3 bucket. Occasionally, third-party tools ingest corrupted images into the S3 bucket. This image corruption causes a poor user experience in the application later. The company has successfully implemented and tested Python logic to detect corrupt images.

A solutions architect must recommend a solution to integrate the detection logic with minimal latency between the ingestion and serving.

Which solution will meet these requirements?

- A. Use a Lambda@Edge function that is invoked by a viewer-response event.
- B. Use a Lambda@Edge function that is invoked by an origin-response event.
- C. Use an S3 event notification that invokes an AWS Lambda function.
- D. Use an S3 event notification that invokes an AWS Step Functions state machine.

**Answer: B**

**Explanation:**

This solution will allow the detection logic to be run as soon as the image is uploaded to the S3 bucket, before it is served to users via the CloudFront distribution. This way, the detection logic can quickly identify any corrupted images and prevent them from being served to users, minimizing latency between ingestion and serving.

Reference: AWS Lambda@Edge documentation:

<https://docs.aws.amazon.com/lambda/latest/dg/lambda-edge.html> You can use Lambda@Edge to run your code in response to CloudFront events, such as a viewer request, an origin request, a response, or an error.

**NEW QUESTION 10**

- (Exam Topic 2)

A company is running an application that uses an Amazon ElastiCache for Redis cluster as a caching layer. A recent security audit revealed that the company has configured encryption at rest for ElastiCache. However, the company did not configure ElastiCache to use encryption in transit. Additionally, users can access the cache without authentication.

A solutions architect must make changes to require user authentication and to ensure that the company is using end-to-end encryption.

Which solution will meet these requirements?

- A. Create an AUTH token. Store the token in AWS System Manager Parameter Store, as an encrypted parameter. Create a new cluster with AUTH and configure encryption in transit. Update the application to retrieve the AUTH token from Parameter Store when necessary and to use the AUTH token for authentication.
- B. Create an AUTH token. Store the token in AWS Secrets Manager. Configure the existing cluster to use the AUTH token and configure encryption in transit. Update the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication.
- C. Create an SSL certificate. Store the certificate in AWS Secrets Manager. Create a new cluster and configure encryption in transit. Update the application to retrieve the SSL certificate from Secrets Manager when necessary and to use the certificate for authentication.
- D. Create an SSL certificate. Store the certificate in AWS Systems Manager Parameter Store, as an encrypted advanced parameter. Update the existing cluster to configure encryption in transit. Update the application to retrieve the SSL certificate from Parameter Store when necessary and to use the certificate for authentication.

**Answer: B**

**Explanation:**

Creating an AUTH token and storing it in AWS Secrets Manager and configuring the existing cluster to use the AUTH token and configure encryption in transit, and updating the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication, would meet the requirements for user authentication and end-to-end encryption.

AWS Secrets Manager is a service that enables you to easily rotate, manage, and retrieve database credentials, API keys, and other secrets throughout their lifecycle. Secrets Manager also enables you to encrypt the data and ensure that only authorized users and applications can access it.

By configuring the existing cluster to use the AUTH token and encryption in transit, all data will be encrypted as it is sent over the network, providing additional security for the data stored in ElastiCache.

Additionally, by updating the application to retrieve the AUTH token from Secrets Manager when necessary and to use the AUTH token for authentication, it ensures that only authorized users and applications can access the cache.

Reference:

AWS Secrets Manager documentation: <https://aws.amazon.com/secrets-manager/> Encryption in transit for ElastiCache:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/encryption.html>

Authentication and Authorization for ElastiCache: <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/accessing-elasticache.html>

### NEW QUESTION 10

- (Exam Topic 2)

A company is using AWS Organizations to manage multiple AWS accounts. For security purposes, the company requires the creation of an Amazon Simple Notification Service (Amazon SNS) topic that enables integration with a third-party alerting system in all the Organizations member accounts.

A solutions architect used an AWS CloudFormation template to create the SNS topic and stack sets to automate the deployment of Cloud Formation stacks.

Trusted access has been enabled in Organizations.

What should the solutions architect do to deploy the CloudFormation StackSets in all AWS accounts?

- A. Create a stack set in the Organizations member account
- B. Use service-managed permission
- C. Set deployment options to deploy to an organizatio
- D. Use CloudFormation StackSets drift detection.
- E. Create stacks in the Organizations member account
- F. Use self-service permission
- G. Set deploymentoptions to deploy to an organizatio
- H. Enable the CloudFormation StackSets automatic deployment.
- I. Create a stack set in the Organizations management accoun
- J. Use service-managed permission
- K. Set deployment options to deploy to the organizatio
- L. Enable CloudFormation StackSets automatic deployment.
- M. Create stacks in the Organizations management accoun
- N. Use service-managed permission
- O. Set deployment options to deploy to the organizatio
- P. Enable CloudFormation StackSets drift detection.

**Answer: C**

#### Explanation:

<https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/stacksets-orgs-manage-auto-deployment.h>

### NEW QUESTION 13

- (Exam Topic 2)

A solutions architect is planning to migrate critical Microsoft SQL Server databases to AWS. Because the databases are legacy systems, the solutions architect will move the databases to a modern data architecture. The solutions architect must migrate the databases with near-zero downtime.

Which solution will meet these requirements?

- A. Use AWS Application Migration Service and the AWS Schema Conversion Tool (AWS SCT). Perform an In-place upgrade before the migratio
- B. Export the migrated data to Amazon Aurora Serverless after cutove
- C. Repoint the applications to Amazon Aurora.
- D. Use AWS Database Migration Service (AWS DMS) to Rehost the databas
- E. Set Amazon S3 as a target.Set up change data capture (CDC) replicatio
- F. When the source and destination are fully synchronized, load the data from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB Instance.
- G. Use native database high availability tools Connect the source system to an Amazon RDS for Microsoft SQL Server DB instance Configure replication accordingl
- H. When data replication is finished, transition the workload to an Amazon RDS for Microsoft SQL Server DB instance.
- I. Use AWS Application Migration Servic
- J. Rehost the database server on Amazon EC2. When data replication is finished, detach the database and move the database to an Amazon RDS for Microsoft SQL Server DB instanc
- K. Reattach the database and then cut over all networking.

**Answer: B**

#### Explanation:

AWS DMS can migrate data from a source database to a target database in AWS, using change data capture (CDC) to replicate ongoing changes and keep the databases in sync. Setting Amazon S3 as a target allows storing the migrated data in a durable and cost-effective storage service. When the source and destination are fully synchronized, the data can be loaded from Amazon S3 into an Amazon RDS for Microsoft SQL Server DB instance, which is a managed database service that simplifies database administration tasks. References:

- [https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Source.SQLServer.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Source.SQLServer.html)
- [https://docs.aws.amazon.com/dms/latest/userguide/CHAP\\_Target.S3.html](https://docs.aws.amazon.com/dms/latest/userguide/CHAP_Target.S3.html)
- [https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_SQLServer.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_SQLServer.html)

### NEW QUESTION 16

- (Exam Topic 2)

A company has a new application that needs to run on five Amazon EC2 instances in a single AWS Region. The application requires high-through put. low-latency network connections between all to the EC2 instances where the application will run. There is no requirement for the application to be fault tolerant.

Which solution will meet these requirements?

- A. Launch five new EC2 instances into a cluster placement grou
- B. Ensure that the EC2 instance type supports enhanced networking.
- C. Launch five new EC2 instances into an Auto Scaling group in the same Availability Zon
- D. Attach an extra elastic network interface to each EC2 instance.
- E. Launch five new EC2 instances into a partition placement grou

- F. Ensure that the EC2 instance type supports enhanced networking.
- G. Launch five new EC2 instances into a spread placement group Attach an extra elastic network interface to each EC2 instance.

**Answer:** A

**Explanation:**

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html#placement-groups-cluster>

**NEW QUESTION 21**

- (Exam Topic 2)

A company is updating an application that customers use to make online orders. The number of attacks on the application by bad actors has increased recently. The company will host the updated application on an Amazon Elastic Container Service (Amazon ECS) cluster. The company will use Amazon DynamoDB to store application data. A public Application Load Balancer (ALB) will provide end users with access to the application. The company must prevent prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack.

Which combination of steps will meet these requirements MOST cost-effectively? (Select TWO.)

- A. Create an Amazon CloudFront distribution with the ALB as the origi
- B. Add a custom header and random value on the CloudFront domai
- C. Configure the ALB to conditionally forward traffic if the header and value match.
- D. Deploy the application in two AWS Region
- E. Configure Amazon Route 53 to route to both Regions with equal weight.
- F. Configure auto scaling for Amazon ECS task
- G. Create a DynamoDB Accelerator (DAX) cluster.
- H. Configure Amazon ElastiCache to reduce overhead on DynamoDB.
- I. Deploy an AWS WAF web ACL that includes an appropriate rule grou
- J. Associate the web ACL with the Amazon CloudFront distribution.

**Answer:** AE

**Explanation:**

The company should create an Amazon CloudFront distribution with the ALB as the origin. The company should add a custom header and random value on the CloudFront domain. The company should configure the ALB to conditionally forward traffic if the header and value match. The company should also deploy an AWS WAF web ACL that includes an appropriate rule group. The company should associate the web ACL with the Amazon CloudFront distribution. This solution will meet the requirements most cost-effectively because Amazon CloudFront is a fast content delivery network (CDN) service that securely delivers data, videos, applications, and APIs to customers globally with low latency, high transfer speeds, all within a developer-friendly environment<sup>1</sup>. By creating an Amazon CloudFront distribution with the ALB as the origin, the company can improve the performance and availability of its application by caching static content at edge locations closer to end users. By adding a custom header and random value on the CloudFront domain, the company can prevent direct access to the ALB and ensure that only requests from CloudFront are forwarded to the ECS tasks. By configuring the ALB to conditionally forward traffic if the header and value match, the company can implement origin access identity (OAI) for its ALB origin. OAI is a feature that enables you to restrict access to your content by requiring users to access your content through CloudFront URLs<sup>2</sup>. By deploying an AWS WAF web ACL that includes an appropriate rule group, the company can prevent attacks and ensure business continuity with minimal service interruptions during an ongoing attack. AWS WAF is a web application firewall that lets you monitor and control web requests that are forwarded to your web applications. You can use AWS WAF to define customizable web security rules that control which traffic can access your web applications and which traffic should be blocked<sup>3</sup>. By associating the web ACL with the Amazon CloudFront distribution, the company can apply the web security rules to all requests that are forwarded by CloudFront.

The other options are not correct because:

- Deploying the application in two AWS Regions and configuring Amazon Route 53 to route to both Regions with equal weight would not prevent attacks or ensure business continuity. Amazon Route 53 is a highly available and scalable cloud Domain Name System (DNS) web service that routes end users to Internet applications by translating names like [www.example.com](http://www.example.com) into numeric IP addresses<sup>4</sup>. However, routing traffic to multiple Regions would not protect against attacks or provide failover in case of an outage. It would also increase operational complexity and costs compared to using CloudFront and AWS WAF.
- Configuring auto scaling for Amazon ECS tasks and creating a DynamoDB Accelerator (DAX) cluster would not prevent attacks or ensure business continuity. Auto scaling is a feature that enables you to automatically adjust your ECS tasks based on demand or a schedule. DynamoDB Accelerator (DAX) is a fully managed, highly available, in-memory cache for DynamoDB that delivers up to a 10x performance improvement. However, these features would not protect against attacks or provide failover in case of an outage. They would also increase operational complexity and costs compared to using CloudFront and AWS WAF.
- Configuring Amazon ElastiCache to reduce overhead on DynamoDB would not prevent attacks or ensure business continuity. Amazon ElastiCache is a fully managed in-memory data store service that makes it easy to deploy, operate, and scale popular open-source compatible in-memory data stores. However, this service would not protect against attacks or provide failover in case of an outage. It would also increase operational complexity and costs compared to using CloudFront and AWS WAF.

References:

- <https://aws.amazon.com/cloudfront/>
- <https://aws.amazon.com/waf/>
- <https://aws.amazon.com/route53/>
- <https://aws.amazon.com/dynamodb/dax/>
- <https://aws.amazon.com/elasticache/>

**NEW QUESTION 24**

- (Exam Topic 2)

A company is creating a REST API to share information with six of its partners based in the United States. The company has created an Amazon API Gateway Regional endpoint. Each of the six partners will access the API once per day to post daily sales figures.

After initial deployment, the company observes 1.000 requests per second originating from 500 different IP addresses around the world. The company believes this traffic is originating from a botnet and wants to secure its API while minimizing cost.

Which approach should the company take to secure its API?

- A. Create an Amazon CloudFront distribution with the API as the origi
- B. Create an AWS WAF web ACL with a rule lo block clients thai submit more than fiverequests per da
- C. Associate the web ACL with the CloudFront distnbutio
- D. Configure CloudFront with an origin access identity (OAI) and associate it with the distributio
- E. Configure API Gateway to ensure only the OAI can run the POST method.

- F. Create an Amazon CloudFront distribution with the API as the origin.
- G. Create an AWS WAF web ACL with a rule to block clients that submit more than five requests per day.
- H. Associate the web ACL with the CloudFront distribution.
- I. Add a custom header to the CloudFront distribution populated with an API key.
- J. Configure the API to require an API key on the POST method.
- K. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API.
- L. Create a resource policy with a request limit and associate it with the API.
- M. Configure the API to require an API key on the POST method.
- N. Create an AWS WAF web ACL with a rule to allow access to the IP addresses used by the six partners. Associate the web ACL with the API.
- O. Create a usage plan with a request limit and associate it with the API.
- P. Create an API key and add it to the usage plan.

**Answer: D**

**Explanation:**

"A usage plan specifies who can access one or more deployed API stages and methods—and also how much and how fast they can access them. The plan uses API keys to identify API clients and meters access to the associated API stages for each key. It also lets you configure throttling limits and quota limits that are enforced on individual client API keys."

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-api-usage-plans.html>

A rate-based rule tracks the rate of requests for each originating IP address, and triggers the rule action on IPs with rates that go over a limit. You set the limit as the number of requests per 5-minute time span..... The following caveats apply to AWS WAF rate-based rules: The minimum rate that you can set is 100. AWS WAF checks the rate of requests every 30 seconds, and counts requests for the prior five minutes each time. Because of this, it's possible for an IP address to send requests at too high a rate for 30 seconds before AWS WAF detects and blocks it. AWS WAF can block up to 10,000 IP addresses. If more than 10,000 IP addresses send high rates of requests at the same time, AWS WAF will only block 10,000 of them. " <https://docs.aws.amazon.com/waf/latest/developerguide/waf-rule-statement-type-rate-based.html>

**NEW QUESTION 27**

- (Exam Topic 2)

A company has multiple business units that each have separate accounts on AWS. Each business unit manages its own network with several VPCs that have CIDR ranges that overlap. The company's marketing team has created a new internal application and wants to make the application accessible to all the other business units. The solution must use private IP addresses only.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Instruct each business unit to add a unique secondary CIDR range to the business unit's VPC.
- B. Peer the VPCs and use a private NAT gateway in the secondary range to route traffic to the marketing team.
- C. Create an Amazon EC2 instance to serve as a virtual appliance in the marketing account's VPC.
- D. Create an AWS Site-to-Site VPN connection between the marketing team and each business unit's VPC.
- E. Perform NAT where necessary.
- F. Create an AWS PrivateLink endpoint service to share the marketing application.
- G. Grant permission to specific AWS accounts to connect to the service.
- H. Create interface VPC endpoints in other accounts to access the application by using private IP addresses.
- I. Create a Network Load Balancer (NLB) in front of the marketing application in a private subnet.
- J. Create an API Gateway API.
- K. Use the Amazon API Gateway private integration to connect the API to the NLB.
- L. Activate IAM authorization for the API.
- M. Grant access to the accounts of the other business units.

**Answer: C**

**Explanation:**

With AWS PrivateLink, the marketing team can create an endpoint service to share their internal application with other accounts securely using private IP addresses. They can grant permission to specific AWS accounts to connect to the service and create interface VPC endpoints in the other accounts to access the application by using private IP addresses. This option does not require any changes to the network of the other business units, and it does not require peering or NATing. This solution is both scalable and secure.

<https://aws.amazon.com/blogs/networking-and-content-delivery/connecting-networks-with-overlapping-ip-range>

**NEW QUESTION 32**

- (Exam Topic 2)

A company has an on-premises Microsoft SQL Server database that writes a nightly 200 GB export to a local drive. The company wants to move the backups to more robust cloud storage on Amazon S3. The company has set up a 10 Gbps AWS Direct Connect connection between the on-premises data center and AWS. Which solution meets these requirements MOST cost-effectively?

- A. Create a new S3 bucket.
- B. Deploy an AWS Storage Gateway file gateway within the VPC that is connected to the Direct Connect connection.
- C. Create a new SMB file share.
- D. Write nightly database exports to the new SMB file share.
- E. Create an Amazon FSx for Windows File Server Single-AZ file system within the VPC that is connected to the Direct Connect connection.
- F. Create a new SMB file share.
- G. Write nightly database exports to an SMB file share on the Amazon FSx file system.
- H. Enable nightly backups.
- I. Create an Amazon FSx for Windows File Server Multi-AZ file system within the VPC that is connected to the Direct Connect connection.
- J. Create a new SMB file share.
- K. Write nightly database exports to an SMB file share on the Amazon FSx file system.
- L. Enable nightly backups.
- M. Create a new S3 bucket.
- N. Deploy an AWS Storage Gateway volume gateway within the VPC that is connected to the Direct Connect connection.
- O. Create a new SMB file share.
- P. Write nightly database exports to the new SMB file share on the volume gateway, and automate copies of this data to an S3 bucket.

**Answer: A**

**Explanation:**

<https://docs.aws.amazon.com/filegateway/latest/files3/CreatingAnSMBFileShare.html>

**NEW QUESTION 37**

- (Exam Topic 2)

A company is running a containerized application in the AWS Cloud. The application is running by using Amazon Elastic Container Service (Amazon ECS) on a set of Amazon EC2 instances. The EC2 instances run in an Auto Scaling group.

The company uses Amazon Elastic Container Registry (Amazon ECR) to store its container images. When a new image version is uploaded, the new image version receives a unique tag.

The company needs a solution that inspects new image versions for common vulnerabilities and exposures. The solution must automatically delete new image tags that have Critical or High severity findings. The solution also must notify the development team when such a deletion occurs.

Which solution meets these requirements?

- A. Configure scan on push on the repository Use Amazon EventBridge to invoke an AWS Step Functions state machine when a scan is complete for images that have Critical or High severity finding
- B. Use the Step Functions state machine to delete the image tag for those images and to notify the development team through Amazon Simple Notification Service (Amazon SNS).
- C. Configure scan on push on the repository Configure scan results to be pushed to an Amazon Simple Queue Service (Amazon SQS) queue
- D. Invoke an AWS Lambda function when a new message is added to the SQS queue
- E. Use the Lambda function to delete the image tag for images that have Critical or High severity finding
- F. Notify the development team by using Amazon Simple Email Service (Amazon SES).
- G. Schedule an AWS Lambda function to start a manual image scan every hour
- H. Configure Amazon EventBridge to invoke another Lambda function when a scan is complete
- I. Use the second Lambda function to delete the image tag for images that have Critical or High severity finding
- J. Notify the development team by using Amazon Simple Notification Service (Amazon SNS).
- K. Configure periodic image scan on the repository
- L. Configure scan results to be added to an Amazon Simple Queue Service (Amazon SQS) queue
- M. Invoke an AWS Step Functions state machine when a new message is added to the SQS queue
- N. Use the Step Functions state machine to delete the image tag for images that have Critical or High severity finding
- O. Notify the development team by using Amazon Simple Email Service (Amazon SES).

**Answer: A**

**Explanation:**

<https://docs.aws.amazon.com/AmazonECR/latest/userguide/ecr-eventbridge.html> "Activating an AWS Step Functions state machine"

<https://docs.aws.amazon.com/step-functions/latest/dg/tutorial-creating-lambda-state-machine.html>

**NEW QUESTION 38**

- (Exam Topic 2)

A company runs an application in an on-premises data center. The application gives users the ability to upload media files. The files persist in a file server. The web application has many users. The application server is overutilized, which causes data uploads to fail occasionally. The company frequently adds new storage to the file server. The company wants to resolve these challenges by migrating the application to AWS.

Users from across the United States and Canada access the application. Only authenticated users should have the ability to access the application to upload files. The company will consider a solution that refactors the application, and the company needs to accelerate application development.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instance
- B. Use an Application Load Balancer to distribute the request
- C. Modify the application to use Amazon S3 to persist the file
- D. Use Amazon Cognito to authenticate users.
- E. Use AWS Application Migration Service to migrate the application server to Amazon EC2 instances. Create an Auto Scaling group for the EC2 instance
- F. Use an Application Load Balancer to distribute the request
- G. Set up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application
- H. Modify the application to use Amazon S3 to persist the files.
- I. Create a static website for uploads of media file
- J. Store the static assets in Amazon S3. Use AWS AppSync to create an API
- K. Use AWS Lambda resolvers to upload the media files to Amazon S3. Use Amazon Cognito to authenticate users.
- L. Use AWS Amplify to create a static website for uploads of media file
- M. Use Amplify Hosting to serve the website through Amazon CloudFront
- N. Use Amazon S3 to store the uploaded media file
- O. Use Amazon Cognito to authenticate users.

**Answer: D**

**Explanation:**

The company should use AWS Amplify to create a static website for uploads of media files. The company should use Amplify Hosting to serve the website through Amazon CloudFront. The company should use Amazon S3 to store the uploaded media files. The company should use Amazon Cognito to authenticate users.

This solution will meet the requirements with the least operational overhead because AWS Amplify is a complete solution that lets frontend web and mobile developers easily build, ship, and host full-stack applications on AWS, with the flexibility to leverage the breadth of AWS services as use cases evolve. No cloud expertise needed<sup>1</sup>. By using AWS Amplify, the company can refactor the application to a serverless architecture that reduces operational complexity and costs.

AWS Amplify offers the following features and benefits:

- Amplify Studio: A visual interface that enables you to build and deploy a full-stack app quickly, including frontend UI and backend.
- Amplify CLI: A local toolchain that enables you to configure and manage an app backend with just a few commands.
- Amplify Libraries: Open-source client libraries that enable you to build cloud-powered mobile and web apps.
- Amplify UI Components: Open-source design system with cloud-connected components for building feature-rich apps fast.
- Amplify Hosting: Fully managed CI/CD and hosting for fast, secure, and reliable static and server-side rendered apps.

By using AWS Amplify to create a static website for uploads of media files, the company can leverage Amplify Studio to visually build a pixel-perfect UI and connect it to a cloud backend in clicks. By using Amplify Hosting to serve the website through Amazon CloudFront, the company can easily deploy its web app or website to the fast, secure, and reliable AWS content delivery network (CDN), with hundreds of points of presence globally. By using Amazon S3 to store the

uploaded media files, the company can benefit from a highly scalable, durable, and cost-effective object storage service that can handle any amount of data<sup>2</sup>. By using Amazon Cognito to authenticate users, the company can add user sign-up, sign-in, and access control to its web app with a fully managed service that scales to support millions of users<sup>3</sup>.

The other options are not correct because:

➤ Using AWS Application Migration Service to migrate the application server to Amazon EC2 instances would not refactor the application or accelerate development. AWS Application Migration Service (AWS MGN) is a service that enables you to migrate physical servers, virtual machines (VMs), or cloud servers from any source infrastructure to AWS without requiring agents or specialized tools. However, this would not address the challenges of overutilization and data uploads failures. It would also not reduce operational overhead or costs compared to a serverless architecture.

➤ Creating a static website for uploads of media files and using AWS AppSync to create an API would not be as simple or fast as using AWS Amplify. AWS AppSync is a service that enables you to create flexible APIs for securely accessing, manipulating, and combining data from one or more data sources. However, this would require more configuration and management than using Amplify Studio and Amplify Hosting. It would also not provide authentication features like Amazon Cognito.

➤ Setting up AWS IAM Identity Center (AWS Single Sign-On) to give users the ability to sign in to the application would not be as suitable as using Amazon Cognito. AWS Single Sign-On (AWS SSO) is a service that enables you to centrally manage SSO access and user permissions across multiple AWS accounts and business applications. However, this service is designed for enterprise customers who need to manage access for employees or partners across multiple resources. It is not intended for authenticating end users of web or mobile apps.

References:

- <https://aws.amazon.com/amplify/>
- <https://aws.amazon.com/s3/>
- <https://aws.amazon.com/cognito/>
- <https://aws.amazon.com/mgn/>
- <https://aws.amazon.com/appsync/>
- <https://aws.amazon.com/single-sign-on/>

## NEW QUESTION 40

- (Exam Topic 2)

A company operates a proxy server on a fleet of Amazon EC2 instances. Partners in different countries use the proxy server to test the company's functionality. The EC2 instances are running in a VPC. and the instances have access to the internet.

The company's security policy requires that partners can access resources only from domains that the company owns.

Which solution will meet these requirements?

- A. Create an Amazon Route 53 Resolver DNS Firewall domain list that contains the allowed domains. Configure a DNS Firewall rule group with a rule that has a high numeric value that blocks all request
- B. Configure a rule that has a low numeric value that allows requests for domains in the allowed list
- C. Associate the rule group with the VPC.
- D. Create an Amazon Route 53 Resolver DNS Firewall domain list that contains the allowed domains. Configure a Route 53 outbound endpoint
- E. Associate the outbound endpoint with the VP
- F. Associate the domain list with the outbound endpoint.
- G. Create an Amazon Route 53 traffic flow policy to match the allowed domain
- H. Configure the traffic flow policy to forward requests that match to the Route 53 Resolve
- I. Associate the traffic flow policy with the VPC.
- J. Create an Amazon Route 53 outbound endpoint
- K. Associate the outbound endpoint with the VP
- L. Configure a Route 53 traffic flow policy to forward requests for allowed domains to the outbound endpoint
- M. Associate the traffic flow policy with the VPC.

**Answer:** A

### Explanation:

The company should create an Amazon Route 53 Resolver DNS Firewall domain list that contains the allowed domains. The company should configure a DNS Firewall rule group with a rule that has a high numeric value that blocks all requests. The company should configure a rule that has a low numeric value that allows requests for domains in the allowed list. The company should associate the rule group with the VPC. This solution will meet the requirements because Amazon Route 53 Resolver DNS Firewall is a feature that enables you to filter and regulate outbound DNS traffic for your VPC. You can create reusable collections of filtering rules in DNS Firewall rule groups and associate them with your VPCs. You can specify lists of domain names to allow or block, and you can customize the responses for the DNS queries that you block<sup>1</sup>. By creating a domain list with the allowed domains and a rule group with rules to allow or block requests based on the domain list, the company can enforce its security policy and control access to sites.

The other options are not correct because:

➤ Configuring a Route 53 outbound endpoint and associating it with the VPC would not help with filtering outbound DNS traffic. A Route 53 outbound endpoint is a resource that enables you to forward DNS queries from your VPC to your network over AWS Direct Connect or VPN connections<sup>2</sup>. It does not provide any filtering capabilities.

➤ Creating a Route 53 traffic flow policy to match the allowed domains would not help with filtering outbound DNS traffic. A Route 53 traffic flow policy is a resource that enables you to route traffic based on multiple criteria, such as endpoint health, geographic location, and latency<sup>3</sup>. It does not provide any filtering capabilities.

➤ Creating a Gateway Load Balancer (GWLB) would not help with filtering outbound DNS traffic. A GWLB is a service that enables you to deploy, scale, and manage third-party virtual appliances such as firewalls, intrusion detection and prevention systems, and deep packet inspection systems in the cloud<sup>4</sup>. It does not provide any filtering capabilities.

References:

- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-dns-firewall.html>
- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/resolver-outbound-endpoints.html>
- <https://docs.aws.amazon.com/Route53/latest/DeveloperGuide/traffic-flow.html>
- <https://docs.aws.amazon.com/elasticloadbalancing/latest/gateway/introduction.html>

## NEW QUESTION 43

- (Exam Topic 2)

A company runs an intranet application on premises. The company wants to configure a cloud backup of the application. The company has selected AWS Elastic

Disaster Recovery for this solution.

The company requires that replication traffic does not travel through the public internet. The application also must not be accessible from the internet. The company does not want this solution to consume all available network bandwidth because other applications require bandwidth.

Which combination of steps will meet these requirements? (Select THREE.)

- A. Create a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway.
- B. Create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway.
- C. Create an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network.
- D. Create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network.
- E. During configuration of the replication servers, select the option to use private IP addresses for data replication.
- F. During configuration of the launch settings for the target servers, select the option to ensure that the Recovery instance's private IP address matches the source server's private IP address.

**Answer:** BDE

**Explanation:**

AWS Elastic Disaster Recovery (AWS DRS) is a service that minimizes downtime and data loss with fast, reliable recovery of on-premises and cloud-based applications using affordable storage, minimal compute, and point-in-time recovery<sup>1</sup>. Users can set up AWS DRS on their source servers to initiate secure data replication to a staging area subnet in their AWS account, in the AWS Region they select. Users can then launch recovery instances on AWS within minutes, using the most up-to-date server state or a previous point in time.

To configure a cloud backup of the application with AWS DRS, users need to create a VPC that has at least two public subnets, a virtual private gateway, and an internet gateway. A VPC is a logically isolated section of the AWS Cloud where users can launch AWS resources in a virtual network that they define<sup>2</sup>. A public subnet is a subnet that has a route to an internet gateway<sup>3</sup>. A virtual private gateway is the VPN concentrator on the Amazon side of the Site-to-Site VPN connection<sup>4</sup>. An internet gateway is a horizontally scaled, redundant, and highly available VPC component that allows communication between instances in the VPC and the internet. Users need to create at least two public subnets for redundancy and high availability. Users need to create a virtual private gateway and attach it to the VPC to enable VPN connectivity between the on-premises network and the target AWS network. Users need to create an internet gateway and attach it to the VPC to enable internet access for the replication servers.

To ensure that replication traffic does not travel through the public internet, users need to create an AWS Direct Connect connection and a Direct Connect gateway between the on-premises network and the target AWS network. AWS Direct Connect is a service that establishes a dedicated network connection from an on-premises network to one or more VPCs. A Direct Connect gateway is a globally available resource that allows users to connect multiple VPCs across different Regions to their on-premises networks using one or more Direct Connect connections. Users need to create an AWS Direct Connect connection between their on-premises network and an AWS Region. Users need to create a Direct Connect gateway and associate it with their VPC and their Direct Connect connection.

To ensure that the application is not accessible from the internet, users need to select the option to use private IP addresses for data replication during configuration of the replication servers. This option configures the replication servers with private IP addresses only, without assigning any public IP addresses or Elastic IP addresses. This way, the replication servers can only communicate with other resources within the VPC or through VPN connections.

Option A is incorrect because creating a VPC that has at least two private subnets, two NAT gateways, and a virtual private gateway is not necessary or cost-effective. A private subnet is a subnet that does not have a route to an internet gateway<sup>3</sup>. A NAT gateway is a highly available, managed Network Address Translation (NAT) service that enables instances in a private subnet to connect to the internet or other AWS services, but prevents the internet from initiating connections with those instances. Users do not need to create private subnets or NAT gateways for this use case, as they can use public subnets with private IP addresses for data replication.

Option C is incorrect because creating an AWS Site-to-Site VPN connection between the on-premises network and the target AWS network will not ensure that replication traffic does not travel through the public

internet. A Site-to-Site VPN connection consists of two VPN tunnels between an on-premises customer gateway device and a virtual private gateway in your VPC<sup>4</sup>. The VPN tunnels are encrypted using IPsec protocols, but they still use public IP addresses for communication. Users need to use AWS Direct Connect instead of Site-to-Site VPN for this use case.

Option F is incorrect because selecting the option to ensure that the Recovery instance's private IP address matches the source server's private IP address during configuration of the launch settings for the target servers will not ensure that the application is not accessible from the internet. This option configures the Recovery instance with an identical private IP address as its source server when launched in drills or recovery mode. However, this option does not prevent assigning public IP addresses or Elastic IP addresses to the Recovery instance. Users need to select the option to use private IP addresses for data replication instead.

**NEW QUESTION 48**

- (Exam Topic 2)

A company plans to migrate a three-tiered web application from an on-premises data center to AWS. The company developed the UI by using server-side JavaScript libraries. The business logic and API tier uses a Python-based web framework. The data tier runs on a MySQL database.

The company custom built the application to meet business requirements. The company does not want to re-architect the application. The company needs a solution to replatform the application to AWS with the least possible amount of development. The solution needs to be highly available and must reduce operational overhead.

Which solution will meet these requirements?

- A. Deploy the UI to a static website on Amazon S3. Use Amazon CloudFront to deliver the website. Build the business logic in a Docker image. Store the image in Amazon Elastic Container Registry (Amazon ECR). Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the website with an Application Load Balancer in front. Deploy the datalayer to an Amazon Aurora MySQL DB cluster.
- B. Build the UI and business logic in Docker images. Store the images in Amazon Elastic Container Registry (Amazon ECR). Use Amazon Elastic Container Service (Amazon ECS) with the Fargate launch type to host the UI and business logic applications with an Application Load Balancer in front. Migrate the database to an Amazon RDS for MySQL Multi-AZ DB instance.
- C. Deploy the UI to a static website on Amazon S3. Use Amazon CloudFront to deliver the website. Convert the business logic to AWS Lambda functions. Integrate the functions with Amazon API Gateway. Deploy the data layer to an Amazon Aurora MySQL DB cluster.
- D. Build the UI and business logic in Docker images. Store the images in Amazon Elastic Container Registry (Amazon ECR). Use Amazon Elastic Kubernetes Service (Amazon EKS) with Fargate profiles to host the UI and business logic. Use AWS Database Migration Service (AWS DMS) to migrate the data layer to Amazon DynamoDB.

**Answer:** A

**Explanation:**

This solution utilizes Amazon S3 and CloudFront to deploy the UI as a static website, which can be done with minimal development effort. The business logic and API tier can be containerized in a Docker image and stored in Amazon Elastic Container Registry (ECR) and run on Amazon Elastic Container Service (ECS) with the Fargate launch type, which allows the application to be highly available with minimal operational overhead. The data layer can be deployed on an Amazon Aurora MySQL DB cluster, which is a fully managed relational database service.

Amazon Aurora provides high availability and performance for the data layer without the need for managing the underlying infrastructure.

**NEW QUESTION 53**

- (Exam Topic 2)

A company needs to architect a hybrid DNS solution. This solution will use an Amazon Route 53 private hosted zone for the domain cloud.example.com for the resources stored within VPCs.

The company has the following DNS resolution requirements:

- On-premises systems should be able to resolve and connect to cloud.example.com.
- All VPCs should be able to resolve cloud.example.com.

There is already an AWS Direct Connect connection between the on-premises corporate network and AWS Transit Gateway. Which architecture should the company use to meet these requirements with the HIGHEST performance?

- A. Associate the private hosted zone to all the VPC
- B. Create a Route 53 inbound resolver in the shared services VP
- C. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.
- D. Associate the private hosted zone to all the VPC
- E. Deploy an Amazon EC2 conditional forwarder in the shared services VP
- F. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the conditional forwarder.
- G. Associate the private hosted zone to the shared services VP
- H. Create a Route 53 outbound resolver in the shared services VP
- I. Attach all VPCs to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the outbound resolver.
- J. Associate the private hosted zone to the shared services VP
- K. Create a Route 53 inbound resolver in the shared services VP
- L. Attach the shared services VPC to the transit gateway and create forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver.

**Answer:** A

**Explanation:**

Amazon Route 53 Resolver is a managed DNS resolver service from Route 53 that helps to create conditional forwarding rules to redirect query traffic<sup>1</sup>. By associating the private hosted zone to all the VPCs, the solutions architect can enable DNS resolution for cloud.example.com within the VPCs. By creating a Route 53 inbound resolver in the shared services VPC, the solutions architect can enable DNS resolution for cloud.example.com from on-premises systems. By attaching all VPCs to the transit gateway, the solutions architect can enable connectivity between the VPCs and the on-premises network through AWS Direct Connect. By creating forwarding rules in the on-premises DNS server for cloud.example.com that point to the inbound resolver, the solutions architect can direct DNS queries for cloud.example.com to the Route 53 Resolver endpoint in AWS. This solution will provide the highest performance as it leverages Route 53 Resolver's optimized routing and caching capabilities.

References: 1: <https://aws.amazon.com/route53/resolver/>

**NEW QUESTION 54**

- (Exam Topic 2)

A company needs to establish a connection from its on-premises data center to AWS. The company needs to connect all of its VPCs that are located in different AWS Regions with transitive routing capabilities between VPC networks. The company also must reduce network outbound traffic costs, increase bandwidth throughput, and provide a consistent network experience for end users.

Which solution will meet these requirements?

- A. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VP
- B. Create VPC peering connections that initiate from the central VPC to all other VPCs.
- C. Create an AWS Direct Connect connection between the on-premises data center and AW
- D. Provision a transit VIF, and connect it to a Direct Connect gateway
- E. Connect the Direct Connect gateway to all the other VPCs by using a transit gateway in each Region.
- F. Create an AWS Site-to-Site VPN connection between the on-premises data center and a new central VP
- G. Use a transit gateway with dynamic routing
- H. Connect the transit gateway to all other VPCs.
- I. Create an AWS Direct Connect connection between the on-premises data center and AWS Establish an AWS Site-to-Site VPN connection between all VPCs in each Region
- J. Create VPC peering connections that initiate from the central VPC to all other VPCs.

**Answer:** B

**Explanation:**

Transit GW + Direct Connect GW + Transit VIF + enabled SiteLink if two different DX locations <https://aws.amazon.com/blogs/networking-and-content-delivery/introducing-aws-direct-connect-sitelink/>

**NEW QUESTION 59**

- (Exam Topic 2)

A company wants to run a custom network analysis software package to inspect traffic as traffic leaves and enters a VPC. The company has deployed the solution by using AWS CloudFormation on three Amazon EC2 instances in an Auto Scaling group. All network routing has been established to direct traffic to the EC2 instances.

Whenever the analysis software stops working, the Auto Scaling group replaces an instance. The network routes are not updated when the instance replacement occurs.

Which combination of steps will resolve this issue? (Select THREE.)

- A. Create alarms based on EC2 status check metrics that will cause the Auto Scaling group to replace the failed instance.
- B. Update the CloudFormation template to install the Amazon CloudWatch agent on the EC2 instances. Configure the CloudWatch agent to send process metrics for the application.
- C. Update the CloudFormation template to install AWS Systems Manager Agent on the EC2 instances. Configure Systems Manager Agent to send process metrics for the application.
- D. Create an alarm for the custom metric in Amazon CloudWatch for the failure scenario
- E. Configure the alarm to publish a message to an Amazon Simple Notification Service (Amazon SNS) topic.
- F. Create an AWS Lambda function that responds to the Amazon Simple Notification Service (Amazon SNS) message to take the instance out of service
- G. Update the network routes to point to the replacement instance.
- H. In the CloudFormation template, write a condition that updates the network routes when a replacement instance is launched.

**Answer:** BDE

#### NEW QUESTION 60

- (Exam Topic 2)

A company has built a high performance computing (HPC) cluster in AWS for a tightly coupled workload that generates a large number of shared files stored in Amazon EFS. The cluster was performing well when the number of Amazon EC2 instances in the cluster was 100. However, when the company increased the cluster size to 1,000 EC2 instances, overall performance was well below expectations.

Which collection of design choices should a solutions architect make to achieve the maximum performance from the HPC cluster? (Select THREE.)

- A. Ensure the HPC cluster is launched within a single Availability Zone.
- B. Launch the EC2 instances and attach elastic network interfaces in multiples of four.
- C. Select EC2 Instance types with an Elastic Fabric Adapter (EFA) enabled.
- D. Ensure the cluster is launched across multiple Availability Zones.
- E. Replace Amazon EFS with multiple Amazon EBS volumes in a RAID array.
- F. Replace Amazon EFS with Amazon FSx for Lustre.

**Answer:** ACF

#### Explanation:

\* A. High performance computing (HPC) workload cluster should be in a single AZ.

\* C. Elastic Fabric Adapter (EFA) is a network device that you can attach to your Amazon EC2 instances to accelerate High Performance Computing (HPC)

\* F. Amazon FSx for Lustre - Use it for workloads where speed matters, such as machine learning, high performance computing (HPC), video processing, and financial modeling.

Cluster – packs instances close together inside an Availability Zone. This strategy enables workloads to achieve the low-latency network performance necessary for tightly-coupled node-to-node communication that is typical of HPC applications.

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/placement-groups.html>

#### NEW QUESTION 63

- (Exam Topic 2)

A company has five development teams that have each created five AWS accounts to develop and host applications. To track spending, the development teams log in to each account every month, record the current cost from the AWS Billing and Cost Management console, and provide the information to the company's finance team.

The company has strict compliance requirements and needs to ensure that resources are created only in AWS Regions in the United States. However, some resources have been created in other Regions.

A solutions architect needs to implement a solution that gives the finance team the ability to track and consolidate expenditures for all the accounts. The solution also must ensure that the company can create resources only in Regions in the United States.

Which combination of steps will meet these requirements in the MOST operationally efficient way? (Select THREE.)

- A. Create a new account to serve as a management account
- B. Create an Amazon S3 bucket for the finance team. Use AWS Cost and Usage Reports to create monthly reports and to store the data in the finance team's S3 bucket.
- C. Create a new account to serve as a management account
- D. Deploy an organization in AWS Organizations with all features enabled
- E. Invite all the existing accounts to the organization
- F. Ensure that each account accepts the invitation.
- G. Create an OU that includes all the development team
- H. Create an SCP that allows the creation of resources only in Regions that are in the United States
- I. Apply the SCP to the OU.
- J. Create an OU that includes all the development team
- K. Create an SCP that denies the creation of resources in Regions that are outside the United States
- L. Apply the SCP to the OU.
- M. Create an IAM role in the management account. Attach a policy that includes permissions to view the Billing and Cost Management console
- N. Allow the finance team users to assume the role
- O. Use AWS Cost Explorer and the Billing and Cost Management console to analyze cost.
- P. Create an IAM role in each AWS account
- Q. Attach a policy that includes permissions to view the Billing and Cost Management console
- R. Allow the finance team users to assume the role.

**Answer:** BCE

#### Explanation:

AWS Organizations is a service that enables you to consolidate multiple AWS accounts into an organization that you create and centrally manage. By creating a management account and inviting all the existing accounts to join the organization, the solutions architect can track and consolidate expenditures for all the accounts using AWS Cost Management tools such as AWS Cost Explorer and AWS Budgets. An organizational unit (OU) is a group of accounts within an organization that can be used to apply policies and simplify management. A service control policy (SCP) is a type of policy that you can use to manage permissions in your organization. By creating an OU that includes all the development teams and applying an SCP that allows the creation of resources only in Regions that are in the United States, the solutions architect can ensure that the company meets its compliance requirements and avoids unwanted charges from other Regions. An IAM role is an identity with permission policies that determine what the identity can and cannot do in AWS. By creating an IAM role in the management account and allowing the finance team users to assume it, the solutions architect can give them access to view the Billing and Cost Management console without sharing credentials or creating additional users. References:

- [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_introduction.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_introduction.html)
- [https://docs.aws.amazon.com/organizations/latest/userguide/orgs\\_manage\\_policies\\_scp.html](https://docs.aws.amazon.com/organizations/latest/userguide/orgs_manage_policies_scp.html)
- [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles.html)
- <https://docs.aws.amazon.com/aws-cost-management/latest/userguide/what-is-costmanagement.html>

#### NEW QUESTION 65

- (Exam Topic 2)

A company needs to audit the security posture of a newly acquired AWS account. The company's data security team requires a notification only when an Amazon

S3 bucket becomes publicly exposed. The company has already established an Amazon Simple Notification Service (Amazon SNS) topic that has the data security team's email address subscribed. Which solution will meet these requirements?

- A. Create an S3 event notification on all S3 buckets for the isPublic even
- B. Select the SNS topic as the target for the event notifications.
- C. Create an analyzer in AWS Identity and Access Management Access Analyze
- D. Create an Amazon EventBridge rule for the event type "Access Analyzer Finding" with a filter for "isPublic: true." Select the SNS topic as the EventBridge rule target.
- E. Create an Amazon EventBridge rule for the event type "Bucket-Level API Call via CloudTrail" with a filter for "PutBucketPolicy." Select the SNS topic as the EventBridge rule target.
- F. Activate AWS Config and add the cloudtrail-s3-dataevents-enabled rul
- G. Create an Amazon EventBridge rule for the event type "Config Rules Re-evaluation Status" with a filter for "NON\_COMPLIANT." Select the SNS topic as the EventBridge rule target.

**Answer: B**

**Explanation:**

Access Analyzer is to assess the access policy. [https://docs.aws.amazon.com/ja\\_jp/AmazonS3/latest/userguide/access-control-block-public-access.html](https://docs.aws.amazon.com/ja_jp/AmazonS3/latest/userguide/access-control-block-public-access.html)

**NEW QUESTION 69**

- (Exam Topic 1)

An application is using an Amazon RDS for MySQL Multi-AZ DB instance in the us-east-1 Region. After a failover test, the application lost the connections to the database and could not re-establish the connections. After a restart of the application, the application re-established the connections.

A solutions architect must implement a solution so that the application can re-establish connections to the database without requiring a restart.

Which solution will meet these requirements?

- A. Create an Amazon Aurora MySQL Serverless v1 DB instanc
- B. Migrate the RDS DB instance to the Aurora Serverless v1 DB instanc
- C. Update the connection settings in the application to point to the Aurora reader endpoint.
- D. Create an RDS prox
- E. Configure the existing RDS endpoint as a targe
- F. Update the connection settings in the application to point to the RDS proxy endpoint.
- G. Create a two-node Amazon Aurora MySQL DB cluste
- H. Migrate the RDS DB instance to the Aurora DB cluste
- I. Create an RDS prox
- J. Configure the existing RDS endpoint as a targe
- K. Update the connection settings in the application to point to the RDS proxy endpoint.
- L. Create an Amazon S3 bucke
- M. Export the database to Amazon S3 by using AWS Database Migration Service (AWS DMS). Configure Amazon Athena to use the S3 bucket as a data stor
- N. Install the latest Open Database Connectivity (ODBC) driver for the applicatio
- O. Update the connection settings in the application to point to the Athena endpoint

**Answer: B**

**Explanation:**

Amazon RDS Proxy is a fully managed database proxy service for Amazon Relational Database Service (RDS) that makes applications more scalable, resilient, and secure. It allows applications to pool and share connections to an RDS database, which can help reduce database connection overhead, improve scalability, and provide automatic failover and high availability.

**NEW QUESTION 73**

- (Exam Topic 1)

A company is refactoring its on-premises order-processing platform in the AWS Cloud. The platform includes a web front end that is hosted on a fleet of VMs RabbitMQ to connect the front end to the backend, and a Kubernetes cluster to run a containerized backend system to process the orders. The company does not want to make any major changes to the application

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- B. Create a custom AWS Lambda runtime to mimic the web server environment Create an Amazon API Gateway API to replace the front-end web servers Set up Amazon MQ to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend
- C. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up Amazon MQ to replace the on-premises messaging queue Install Kubernetes on a fleet of different EC2 instances to host the order-processing backend
- D. Create an AMI of the web server VM Create an Amazon EC2 Auto Scaling group that uses the AMI and an Application Load Balancer Set up an Amazon Simple Queue Service (Amazon SQS) queue to replace the on-premises messaging queue Configure Amazon Elastic Kubernetes Service (Amazon EKS) to host the order-processing backend

**Answer: A**

**Explanation:**

<https://aws.amazon.com/about-aws/whats-new/2020/11/announcing-amazon-mq-rabbitmq/>

**NEW QUESTION 75**

- (Exam Topic 1)

A company uses AWS Organizations for a multi-account setup in the AWS Cloud. The company uses AWS Control Tower for governance and uses AWS Transit Gateway for VPC connectivity across accounts.

In an AWS application account, the company's application team has deployed a web application that uses AWS Lambda and Amazon RDS. The company's database administrators have a separate DBA account and use the account to centrally manage all the databases across the organization. The database administrators use an Amazon EC2 instance that is deployed in the DBA account to access an RDS database that is deployed in the application account.

The application team has stored the database credentials as secrets in AWS Secrets Manager in the application account. The application team is manually sharing

the secrets with the database administrators. The secrets are encrypted by the default AWS managed key for Secrets Manager in the application account. A solutions architect needs to implement a solution that gives the database administrators access to the database and eliminates the need to manually share the secrets.

Which solution will meet these requirements?

- A. Use AWS Resource Access Manager (AWS RAM) to share the secrets from the application account with the DBA account
- B. In the DBA account, create an IAM role that is named DBA-Admi
- C. Grant the role the required permissions to access the shared secret
- D. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- E. In the application account, create an IAM role that is named DBA-Secre
- F. Grant the role the required permissions to access the secret
- G. In the DBA account, create an IAM role that is named DBA-Admi
- H. Grant the DBA-Admin role the required permissions to assume the DBA-Secret role in the application account
- I. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- J. In the DBA account, create an IAM role that is named DBA-Admi
- K. Grant the role the required permissions to access the secrets and the default AWS managed key in the application account
- L. In the application account, attach resource-based policies to the key to allow access from the DBA account
- M. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.
- N. In the DBA account, create an IAM role that is named DBA-Admi
- O. Grant the role the required permissions to access the secrets in the application account
- P. Attach an SCP to the application account to allow access to the secrets from the DBA account
- Q. Attach the DBA-Admin role to the EC2 instance for access to the cross-account secrets.

**Answer:** B

**Explanation:**

➤ Option B is correct because creating an IAM role in the application account that has permissions to access the secrets and creating an IAM role in the DBA account that has permissions to assume the role in the application account eliminates the need to manually share the secrets. This approach uses cross-account IAM roles to grant access to the secrets in the application account. The database administrators can assume the role in the application account from their EC2 instance in the DBA

account and retrieve the secrets without having to store them locally or share them manually2

References: 1: <https://docs.aws.amazon.com/ram/latest/userguide/what-is.html> 2:

[https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial\\_cross-account-with-roles.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/tutorial_cross-account-with-roles.html) 3:

<https://docs.aws.amazon.com/kms/latest/developerguide/concepts.html> : [https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials\\_basic.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/tutorials_basic.html) :

<https://docs.aws.amazon.com/IAM/latest/UserGuide/introduction.html>

**NEW QUESTION 79**

- (Exam Topic 1)

A company is hosting a three-tier web application in an on-premises environment. Due to a recent surge in traffic that resulted in downtime and a significant financial impact, company management has ordered that the application be moved to AWS. The application is written in .NET and has a dependency on a MySQL database. A solutions architect must design a scalable and highly available solution to meet the demand of 200,000 daily users.

Which steps should the solutions architect take to design an appropriate solution?

- A. Use AWS Elastic Beanstalk to create a new application with a web server environment and an Amazon RDS MySQL Multi-AZ DB instance. The environment should launch a Network Load Balancer (NLB) in front of an Amazon EC2 Auto Scaling group in multiple Availability Zones. Use an Amazon Route 53 alias record to route traffic from the company's domain to the NLB.
- B. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones.
- C. The stack should launch a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy.
- D. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.
- E. Use AWS Elastic Beanstalk to create an automatically scaling web server environment that spans two separate Regions with an Application Load Balancer (ALB) in each Region.
- F. Create a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a cross-Region read replica. Use Amazon Route 53 with a geoproximity routing policy to route traffic between the two Regions.
- G. Use AWS CloudFormation to launch a stack containing an Application Load Balancer (ALB) in front of an Amazon ECS cluster of Spot Instances spanning three Availability Zones. The stack should launch an Amazon RDS MySQL DB instance with a Snapshot deletion policy. Use an Amazon Route 53 alias record to route traffic from the company's domain to the ALB.

**Answer:** C

**Explanation:**

Using AWS CloudFormation to launch a stack with an Application Load Balancer (ALB) in front of an Amazon EC2 Auto Scaling group spanning three Availability Zones, a Multi-AZ deployment of an Amazon Aurora MySQL DB cluster with a Retain deletion policy, and an Amazon Route 53 alias record to route traffic from the company's domain to the ALB will ensure that

**NEW QUESTION 83**

- (Exam Topic 1)

A company is running applications on AWS in a multi-account environment. The company's sales team and marketing team use separate AWS accounts in AWS Organizations.

The sales team stores petabytes of data in an Amazon S3 bucket. The marketing team uses Amazon QuickSight for data visualizations. The marketing team needs access to data that the sales team stores in the S3 bucket. The company has encrypted the S3 bucket with an AWS Key Management Service (AWS KMS) key. The marketing team has already created the IAM service role for QuickSight to provide QuickSight access in the marketing AWS account. The company needs a solution that will provide secure access to the data in the S3 bucket across AWS accounts.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new S3 bucket in the marketing account
- B. Create an S3 replication rule in the sales account to copy the objects to the new S3 bucket in the marketing account
- C. Update the QuickSight permissions in the marketing account to grant access to the new S3 bucket.
- D. Create an SCP to grant access to the S3 bucket to the marketing account
- E. Use AWS Resource Access Manager (AWS RAM) to share the KMS key from the sales account with the marketing account

- F. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- G. Update the S3 bucket policy in the marketing account to grant access to the QuickSight rol
- H. Create a KMS grant for the encryption key that is used in the S3 bucke
- I. Grant decrypt access to the QuickSight rol
- J. Update the QuickSight permissions in the marketing account to grant access to the S3 bucket.
- K. Create an IAM role in the sales account and grant access to the S3 bucke
- L. From the marketing account, assume the IAM role in the sales account to access the S3 bucke
- M. Update the QuickSight rote, to create a trust relationship with the new IAM role in the sales account.

**Answer:** D

**Explanation:**

Create an IAM role in the sales account and grant access to the S3 bucket. From the marketing account, assume the IAM role in the sales account to access the S3 bucket. Update the QuickSight role, to create a trust relationship with the new IAM role in the sales account.

This approach is the most secure way to grant cross-account access to the data in the S3 bucket while minimizing operational overhead. By creating an IAM role in the sales account, the marketing team can assume the role in their own account, and have access to the S3 bucket. And updating the QuickSight role, to create a trust relationship with the new IAM role in the sales account will grant the marketing team to access the data in the S3 bucket and use it for data visualization using QuickSight.

AWS Resource Access Manager (AWS RAM) also allows sharing of resources between accounts, but it would require additional management and configuration to set up the sharing, which would increase operational overhead.

Using S3 replication would also replicate the data to the marketing account, but it would not provide the marketing team access to the original data, and also it would increase operational overhead with managing the replication process.

IAM roles and policies, KMS grants and trust relationships are a powerful combination for managing cross-account access in a secure and efficient manner. References:

- AWS IAM Roles
- AWS KMS - Key Grants
- AWS RAM

**NEW QUESTION 88**

- (Exam Topic 1)

A company has an application that runs on Amazon EC2 instances. A solutions architect is designing VPC infrastructure in an AWS Region where the application needs to access an Amazon Aurora DB cluster. The EC2 instances are all associated with the same security group. The DB cluster is associated with its own security group.

The solutions architect needs to add rules to the security groups to provide the application with least privilege access to the DB cluster.

Which combination of steps will meet these requirements? (Select TWO.)

- A. Add an inbound rule to the EC2 instances' security grou
- B. Specify the DB cluster's security group as the source over the default Aurora port.
- C. Add an outbound rule to the EC2 instances' security grou
- D. Specify the DB cluster's security group as the destination over the default Aurora port.
- E. Add an inbound rule to the DB cluster's security grou
- F. Specify the EC2 instances' security group as the source over the default Aurora port.
- G. Add an outbound rule to the DB cluster's security grou
- H. Specify the EC2 instances' security group as the destination over the default Aurora port.
- I. Add an outbound rule to the DB cluster's security grou
- J. Specify the EC2 instances' security group as the destination over the ephemeral ports.

**Answer:** AB

**Explanation:**

\* B. Add an outbound rule to the EC2 instances' security group. Specify the DB cluster's security group as the destination over the default Aurora port. This allows the instances to make outbound connections to the DB cluster on the default Aurora port. C. Add an inbound rule to the DB cluster's security group. Specify the EC2 instances' security group as the source over the default Aurora port. This allows connections to the DB cluster from the EC2 instances on the default Aurora port.

**NEW QUESTION 93**

- (Exam Topic 1)

An enterprise company wants to allow its developers to purchase third-party software through AWS Marketplace. The company uses an AWS Organizations account structure with full features enabled, and has a shared services account in each organizational unit (OU) that will be used by procurement managers. The procurement team's policy indicates that developers should be able to obtain third-party software from an approved list only and use Private Marketplace in AWS Marketplace to achieve this requirement . The procurement team wants administration of Private Marketplace to be restricted to a role named procurement-manager-role, which could be assumed by procurement managers Other IAM users groups, roles, and account administrators in the company should be denied Private Marketplace administrative access

What is the MOST efficient way to design an architecture to meet these requirements?

- A. Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the PowerUserAccess managed policy to the role Apply an inline policy to all IAM users and roles in every AWS account to deny permissions on the AWSPrivateMarketplaceAdminFullAccess managed policy.
- B. Create an IAM role named procurement-manager-role in all AWS accounts in the organization Add the AdministratorAccess managed policy to the role Define a permissions boundary with the AWSPrivateMarketplaceAdminFullAccess managed policy and attach it to all the developer roles.
- C. Create an IAM role named procurement-manager-role in all the shared services accounts in the organization Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the role Create an organization root-level SCP to deny permissions to administer Private Marketplace to everyone exceptthe role named procurement-manager-role Create another organization root-level SCP to deny permissions to create an IAM role named procurement-manager-role to everyone in the organization.
- D. Create an IAM role named procurement-manager-role in all AWS accounts that will be used by developer
- E. Add the AWSPrivateMarketplaceAdminFullAccess managed policy to the rol
- F. Create an SCP in Organizations to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-rol
- G. Apply the SCP to all the shared services accounts in the organization.

**Answer:** C

**Explanation:**

SCP to deny permissions to administer Private Marketplace to everyone except the role named procurement-manager-role.

<https://aws.amazon.com/blogs/awsmarketplace/controlling-access-to-a-well-architected-private-marketplace-usi>

This approach allows the procurement managers to assume the procurement-manager-role in shared services accounts, which have the AWSPrivateMarketplaceAdminFullAccess managed policy attached to it and can then manage the Private Marketplace. The organization root-level SCP denies the permission to administer Private Marketplace to everyone except the role named procurement-manager-role and another SCP denies the permission to create an IAM role named procurement-manager-role to everyone in the organization, ensuring that only the procurement team can assume the role and manage the Private Marketplace. This approach provides a centralized way to manage and restrict access to Private Marketplace while maintaining a high level of security.

**NEW QUESTION 98**

- (Exam Topic 1)

A company is subject to regulatory audits of its financial information. External auditors who use a single AWS account need access to the company's AWS account. A solutions architect must provide the auditors with secure, read-only access to the company's AWS account. The solution must comply with AWS security best practices.

Which solution will meet these requirements?

- A. In the company's AWS account, create resource policies for all resources in the account to grant access to the auditors' AWS account
- B. Assign a unique external ID to the resource policy.
- C. In the company's AWS account create an IAM role that trusts the auditors' AWS account Create an IAM policy that has the required permission
- D. Attach the policy to the role
- E. Assign a unique external ID to the role's trust policy.
- F. In the company's AWS account, create an IAM user
- G. Attach the required IAM policies to the IAM user. Create API access keys for the IAM user
- H. Share the access keys with the auditors.
- I. In the company's AWS account, create an IAM group that has the required permissions Create an IAM user in the company's account for each auditor
- J. Add the IAM users to the IAM group.

**Answer: B**

**Explanation:**

This solution will allow the external auditors to have read-only access to the company's AWS account while being compliant with AWS security best practices. By creating an IAM role, which is a secure and flexible way of granting access to AWS resources, and trusting the auditors' AWS account, the company can ensure that the auditors only have the permissions that are required for their role and nothing more. Assigning a unique external ID to the role's trust policy, it will ensure that only the auditors' AWS account can assume the role.

Reference:

AWS IAM Roles documentation: <https://aws.amazon.com/iam/features/roles/> AWS IAM Best practices: <https://aws.amazon.com/iam/security-best-practices/>

**NEW QUESTION 102**

- (Exam Topic 1)

A company developed a pilot application by using AWS Elastic Beanstalk and Java. To save costs during development, the company's development team deployed the application into a single-instance environment. Recent tests indicate that the application consumes more CPU than expected. CPU utilization is regularly greater than 85%, which causes some performance bottlenecks.

A solutions architect must mitigate the performance issues before the company launches the application to production.

Which solution will meet these requirements with the LEAST operational overhead?

- A. Create a new Elastic Beanstalk application
- B. Select a load-balanced environment type
- C. Select all Availability Zones
- D. Add a scale-out rule that will run if the maximum CPU utilization is over 85% for 5 minutes.
- E. Create a second Elastic Beanstalk environment
- F. Apply the traffic-splitting deployment policy
- G. Specify a percentage of incoming traffic to direct to the new environment in the average CPU utilization is over 85% for 5 minutes.
- H. Modify the existing environment's capacity configuration to use a load-balanced environment type. Select all Availability Zones
- I. Add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes.
- J. Select the Rebuild environment action with the load balancing option Select an Availability Zone Add a scale-out rule that will run if the sum CPU utilization is over 85% for 5 minutes.

**Answer: C**

**Explanation:**

This solution will meet the requirements with the least operational overhead because it allows the company to modify the existing environment's capacity configuration, so it becomes a load-balanced environment type. By selecting all availability zones, the company can ensure that the application is running in multiple availability zones, which can help to improve the availability and scalability of the application. The company can also add a scale-out rule that will run if the average CPU utilization is over 85% for 5 minutes, which can help to mitigate the performance issues. This solution does not require creating new Elastic Beanstalk environments or rebuilding the existing one, which reduces the operational overhead.

You can refer to the AWS Elastic Beanstalk documentation for more information on how to use this service: <https://aws.amazon.com/elasticbeanstalk/> You can refer to the AWS documentation for more information on how to use autoscaling: <https://aws.amazon.com/autoscaling/>

**NEW QUESTION 105**

- (Exam Topic 1)

A company gives users the ability to upload images from a custom application. The upload process invokes an AWS Lambda function that processes and stores the image in an Amazon S3 bucket. The application invokes the Lambda function by using a specific function version ARN.

The Lambda function accepts image processing parameters by using environment variables. The company often adjusts the environment variables of the Lambda function to achieve optimal image processing output. The company tests different parameters and publishes a new function version with the updated environment variables after validating results. This update process also requires frequent changes to the custom application to invoke the new function version ARN. These changes cause interruptions for users.

A solutions architect needs to simplify this process to minimize disruption to users. Which solution will meet these requirements with the LEAST operational overhead?

- A. Directly modify the environment variables of the published Lambda function version

- B. Use theSLATEST version to test image processing parameters.
- C. Create an Amazon DynamoDB table to store the image processing parameter
- D. Modify the Lambda function to retrieve the image processing parameters from the DynamoDB table.
- E. Directly code the image processing parameters within the Lambda function and remove the environment variable
- F. Publish a new function version when the company updates the parameters.
- G. Create a Lambda function alia
- H. Modify the client application to use the function alias AR
- I. Reconfigure the Lambda alias to point to new versions of the function when the company finishes testing.

**Answer: D**

**Explanation:**

A Lambda function alias allows you to point to a specific version of a function and also can be updated to point to a new version of the function without modifying the client application. This way, the company can test different versions of the function with different environment variables and, once the optimal parameters are found, update the alias to point to the new version, without the need to update the client application.

By using this approach, the company can simplify the process of updating the environment variables, minimize disruption to users, and reduce the operational overhead.

Reference:

AWS Lambda documentation: <https://aws.amazon.com/lambda/>

AWS Lambda Aliases documentation: <https://docs.aws.amazon.com/lambda/latest/dg/aliases-intro.html> AWS Lambda versioning and aliases documentation: <https://aws.amazon.com/blogs/compute/versioning-aliases-in-aws-lambda/>

**NEW QUESTION 107**

- (Exam Topic 1)

A security engineer determined that an existing application retrieves credentials to an Amazon RDS for MySQL database from an encrypted file in Amazon S3. For the next version of the application, the security engineer wants to implement the following application design changes to improve security:

- The database must use strong, randomly generated passwords stored in a secure AWS managed service.
- The application resources must be deployed through AWS CloudFormation.
- The application must rotate credentials for the database every 90 days.

A solutions architect will generate a CloudFormation template to deploy the application.

Which resources specified in the CloudFormation template will meet the security engineer's requirements with the LEAST amount of operational overhead?

- A. Generate the database password as a secret resource using AWS Secrets Manage
- B. Create an AWS Lambda function resource to rotate the database passwor
- C. Specify a Secrets Manager RotationSchedule resource to rotate the database password every 90 days.
- D. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Stor
- E. Create an AWS Lambda function resource to rotate the database passwor
- F. Specify a Parameter Store RotationSchedule resource to rotate the database password every 90 days.
- G. Generate the database password as a secret resource using AWS Secrets Manage
- H. Create an AWS Lambda function resource to rotate the database passwor
- I. Create an Amazon EventBridge scheduled rule resource to trigger the Lambda function password rotation every 90 days.
- J. Generate the database password as a SecureString parameter type using AWS Systems Manager Parameter Stor
- K. Specify an AWS AppSync DataSource resource to automatically rotate the database password every 90 days.

**Answer: B**

**Explanation:**

<https://aws.amazon.com/blogs/security/how-to-securely-provide-database-credentials-to-lambda-functions-by-us>

<https://docs.aws.amazon.com/secretsmanager/latest/userguide/rotating-secrets.html>

[https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating\\_cloudformation.html](https://docs.aws.amazon.com/secretsmanager/latest/userguide/integrating_cloudformation.html)

**NEW QUESTION 111**

- (Exam Topic 1)

A company runs a Java application that has complex dependencies on VMs that are in the company's data center. The application is stable. but the company wants to modernize the technology stack. The company wants to migrate the application to AWS and minimize the administrative overhead to maintain the servers.

Which solution will meet these requirements with the LEAST code changes?

- A. Migrate the application to Amazon Elastic Container Service (Amazon ECS) on AWS Fargate by using AWS App2Containe
- B. Store container images in Amazon Elastic Container Registry (Amazon ECR). Grant the ECS task execution role permission 10 access the ECR image repositor
- C. Configure Amazon ECS to use an Application Load Balancer (ALB). Use the ALB to interact with the application.
- D. Migrate the application code to a container that runs in AWS Lambd
- E. Build an Amazon API Gateway REST API with Lambda integratio
- F. Use API Gateway to interact with the application.
- G. Migrate the application to Amazon Elastic Kubernetes Service (Amazon EKS) on EKS managed node groups by using AWS App2Containe
- H. Store container images in Amazon Elastic Container Registry (Amazon ECR). Give the EKS nodes permission to access the ECR image repositor
- I. Use Amazon API Gateway to interact with the application.
- J. Migrate the application code to a container that runs in AWS Lambd
- K. Configure Lambda to use an Application Load Balancer (ALB). Use the ALB to interact with the application.

**Answer: A**

**Explanation:**

According to the AWS documentation<sup>1</sup>, AWS App2Container (A2C) is a command line tool for migrating and modernizing Java and .NET web applications into container format. AWS A2C analyzes and builds an inventory of applications running in bare metal, virtual machines, Amazon Elastic Compute Cloud (EC2) instances, or in the cloud. You can use AWS A2C to generate container images for your applications and deploy them on Amazon ECS or Amazon EKS.

Option A meets the requirements of the scenario because it allows you to migrate your existing Java application to AWS and minimize the administrative overhead to maintain the servers. You can use AWS A2C to analyze your application dependencies, extract application artifacts, and generate a Dockerfile. You can then store your container images in Amazon ECR, which is a fully managed container registry service. You can use AWS Fargate as the launch type for your Amazon ECS cluster, which is a serverless compute engine that eliminates the need to provision and manage servers for your containers. You can grant the ECS task

execution role permission to access the ECR image repository, which allows your tasks to pull images from ECR. You can configure Amazon ECS to use an ALB, which is a load balancer that distributes traffic across multiple targets in multiple Availability Zones using HTTP or HTTPS protocols. You can use the ALB to interact with your application.

**NEW QUESTION 113**

- (Exam Topic 1)

A company runs a Python script on an Amazon EC2 instance to process data. The script runs every 10 minutes. The script ingests files from an Amazon S3 bucket and processes the files. On average, the script takes approximately 5 minutes to process each file. The script will not reprocess a file that the script has already processed.

The company reviewed Amazon CloudWatch metrics and noticed that the EC2 instance is idle for approximately 40% of the time because of the file processing speed. The company wants to make the workload highly available and scalable. The company also wants to reduce long-term management overhead.

Which solution will meet these requirements MOST cost-effectively?

- A. Migrate the data processing script to an AWS Lambda function
- B. Use an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects.
- C. Create an Amazon Simple Queue Service (Amazon SQS) queue
- D. Configure Amazon S3 to send event notifications to the SQS queue
- E. Create an EC2 Auto Scaling group with a minimum size of one instance
- F. Update the data processing script to poll the SQS queue
- G. Process the S3 objects that the SQS message identifies.
- H. Migrate the data processing script to a container image
- I. Run the data processing container on an EC2 instance
- J. Configure the container to poll the S3 bucket for new objects and to process the resulting objects.
- K. Migrate the data processing script to a container image that runs on Amazon Elastic Container Service (Amazon ECS) on AWS Fargate
- L. Create an AWS Lambda function that calls the Fargate RunTaskAPI operation when the container processes the file
- M. Use an S3 event notification to invoke the Lambda function.

**Answer: D**

**Explanation:**

migrating the data processing script to an AWS Lambda function and using an S3 event notification to invoke the Lambda function to process the objects when the company uploads the objects. This solution meets the company's requirements of high availability and scalability, as well as reducing long-term management overhead, and is likely to be the most cost-effective option.

**NEW QUESTION 116**

- (Exam Topic 1)

A company is hosting a critical application on a single Amazon EC2 instance. The application uses an Amazon ElastiCache for Redis single-node cluster for an in-memory data store. The application uses an Amazon RDS for MariaDB DB instance for a relational database. For the application to function, each piece of the infrastructure must be healthy and must be in an active state.

A solutions architect needs to improve the application's architecture so that the infrastructure can automatically recover from failure with the least possible downtime.

Which combination of steps will meet these requirements? (Select THREE.)

- A. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances
- B. Ensure that the EC2 instances are part of an Auto Scaling group that has a minimum capacity of two instances.
- C. Use an Elastic Load Balancer to distribute traffic across multiple EC2 instances. Ensure that the EC2 instances are configured in unlimited mode.
- D. Modify the DB instance to create a read replica in the same Availability Zone
- E. Promote the read replica to be the primary DB instance in failure scenarios.
- F. Modify the DB instance to create a Multi-AZ deployment that extends across two Availability Zones.
- G. Create a replication group for the ElastiCache for Redis cluster
- H. Configure the cluster to use an Auto Scaling group that has a minimum capacity of two instances.
- I. Create a replication group for the ElastiCache for Redis cluster
- J. Enable Multi-AZ on the cluster.

**Answer: ADF**

**Explanation:**

➤ Option A is correct because using an Elastic Load Balancer and an Auto Scaling group with a minimum capacity of two instances can improve the availability and scalability of the EC2 instances that host the application. The load balancer can distribute traffic across multiple instances and the Auto Scaling group can replace any unhealthy instances automatically.

➤ Option D is correct because modifying the DB instance to create a Multi-AZ deployment that extends across two Availability Zones can improve the availability and durability of the RDS for MariaDB database. Multi-AZ deployments provide enhanced data protection and minimize downtime by automatically failing over to a standby replica in another Availability Zone in case of a planned or unplanned outage.

➤ Option F is correct because creating a replication group for the ElastiCache for Redis cluster and enabling Multi-AZ on the cluster can improve the availability and fault tolerance of the in-memory data store. A replication group consists of a primary node and up to five read-only replica nodes that are synchronized with the primary node using asynchronous replication. Multi-AZ allows automatic failover to one of the replicas if the primary node fails or becomes unreachable.

References: 1:

<https://docs.aws.amazon.com/elasticloadbalancing/latest/userguide/how-elastic-load-balancing-works.html> 2:

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/burstable-performance-instances-unlimited-mode.html> 3:

[https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER\\_ReadRepl.html](https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/USER_ReadRepl.html) 4:

<https://docs.aws.amazon.com/AmazonRDS/latest/UserGuide/Concepts.MultiAZ.html> 5:

<https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/AutoScaling.html> 6: <https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/Replication.Redis.Groups.html>

**NEW QUESTION 119**

- (Exam Topic 1)

A company is building a software-as-a-service (SaaS) solution on AWS. The company has deployed an Amazon API Gateway REST API with AWS Lambda integration in multiple AWS Regions and in the same production account.

The company offers tiered pricing that gives customers the ability to pay for the capacity to make a certain number of API calls per second. The premium tier offers up to 3,000 calls per second, and customers are identified by a unique API key. Several premium tier customers in various Regions report that they receive error responses of 429 Too Many Requests from multiple API methods during peak usage hours. Logs indicate that the Lambda function is never invoked. What could be the cause of the error messages for these customers?

- A. The Lambda function reached its concurrency limit.
- B. The Lambda function its Region limit for concurrency.
- C. The company reached its API Gateway account limit for calls per second.
- D. The company reached its API Gateway default per-method limit for calls per second.

**Answer:** C

**Explanation:**

<https://docs.aws.amazon.com/apigateway/latest/developerguide/api-gateway-request-throttling.html#apig-reques>

**NEW QUESTION 122**

- (Exam Topic 1)

A company with global offices has a single 1 Gbps AWS Direct Connect connection to a single AWS Region. The company's on-premises network uses the connection to communicate with the company's resources in the AWS Cloud. The connection has a single private virtual interface that connects to a single VPC. A solutions architect must implement a solution that adds a redundant Direct Connect connection in the same Region. The solution also must provide connectivity to other Regions through the same pair of Direct Connect connections as the company expands into other Regions.

Which solution meets these requirements?

- A. Provision a Direct Connect gatewa
- B. Delete the existing private virtual interface from the existing connectio
- C. Create the second Direct Connect connectio
- D. Create a new private virtual interlace on each connection, and connect both private virtual interfaces to the Direct Connect gatewa
- E. Connect the Direct Connect gateway to the single VPC.
- F. Keep the existing private virtual interfac
- G. Create the second Direct Connect connectio
- H. Create a new private virtual interface on the new connection, and connect the new private virtual interface to the single VPC.
- I. Keep the existing private virtual interfac
- J. Create the second Direct Connect connectio
- K. Create a new public virtual interface on the new connection, and connect the new public virtual interface to the single VPC.
- L. Provision a transit gatewa
- M. Delete the existing private virtual interface from the existing connection.Create the second Direct Connect connectio
- N. Create a new private virtual interface on each connection, and connect both private virtual interfaces to the transit gatewa
- O. Associate the transit gateway with the single VPC.

**Answer:** A

**Explanation:**

A Direct Connect gateway is a globally available resource. You can create the Direct Connect gateway in any Region and access it from all other Regions. The following describe scenarios where you can use a Direct Connect gateway.

<https://docs.aws.amazon.com/directconnect/latest/UserGuide/direct-connect-gateways-intro.html>

**NEW QUESTION 126**

.....

## Thank You for Trying Our Product

\* **100% Pass or Money Back**

All our products come with a 90-day Money Back Guarantee.

\* **One year free update**

You can enjoy free update one year. 24x7 online support.

\* **Trusted by Millions**

We currently serve more than 30,000,000 customers.

\* **Shop Securely**

All transactions are protected by VeriSign!

**100% Pass Your AWS-Certified-Solutions-Architect-Professional Exam with Our Prep Materials Via below:**

<https://www.certleader.com/AWS-Certified-Solutions-Architect-Professional-dumps.html>